Gustavo Ponce, Esq.
Nevada Bar No. 15084
Mona Amini, Esq.
Nevada Bar No. 15381
**KAZEROUNI LAW GROUP, APC**
6787 W. Tropicana Avenue, Suite 250
Las Vegas, Nevada 89103
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
E-mail: gustavo@kazlg.com
mona@kazlg.com

*Attorneys for Plaintiff*

**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEVADA**

| | |
|---|---|
| DANNY ALLEN, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>vs.<br><br>NATIONS DIRECT MORTGAGE, LLC,<br><br>Defendant. | Case No.:<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

//

//

//

//

//

//

//

//

## INTRODUCTION

1. Plaintiff Danny Allen ("Plaintiff") individually and on behalf of all others similarly situated (collectively, the "Class members") brings this class action against Nations Direct Mortgage, LLC ("Defendant" or "Nations Direct") for their failure to secure and safeguard his and other similarly situated Class members' personally identifying information ("PII") including but not limited to their name, address, social security number, and unique Nations Direct loan number.

2. On or about December 30, 2023, Nations Direct became aware of unauthorized access to certain systems within its computer information technology network, where an unauthorized third party obtained and removed the data from its systems, which included names, addresses, social security numbers, and unique Nations Direct loan numbers of individuals from across the country (the "Data Breach").

3. On or around March 6, 2024, Defendant sent Plaintiff a "NOTICE OF POTENTIAL DATA BREACH" indicating that an unauthorized party had accessed and removed data certain files from Defendant's systems, which involved Plaintiff's PII data entrusted to Defendant, including Plaintiff's name, address, social security number, and unique Nations Direct loan number.

4. Defendant's NOTICE OF POTENTIAL DATA BREACH did not specify how many individuals were affected by the Data Breach; however, Defendant has announced via its reporting to the Office of the Maine Attorney General[1] that a total of 83,108 individuals nationwide were affected by the Data Breach.

5. Defendant owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing to implement and maintain reasonable security

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1ee1929d-4e0f-4b9e-b202-59cb6d9e567d.shtml (last visited March 26, 2024).

procedures and practices to protect Plaintiff and other similarly situated individuals from unauthorized access and disclosure.

6. As a result of Defendant's inadequate data security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed, obtained, and exfiltrated by unauthorized third parties.

7. Because the Data Breach compromised Plaintiff's sensitive personal information, Plaintiff and the Class (defined below) have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

8. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their PII, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, reviewing, spending time monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites or accounts.

9. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII was accessed, obtained, and exfiltrated as a result of the Data Breach, which occurred on or around December 30, 2023.

## JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendant; and (4) the Defendant is not a government entity.

11. This Court has personal jurisdiction over Defendant because it is a limited liability company which maintains a headquarters and/or principal place of business in the Henderson, Nevada, and regularly conducts business nationwide and within this district.

12. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District and because Defendant resides and/or are registered to do business and transact business within this District.

**PARTIES**

13. Plaintiff is a resident and citizen of the State of California. Defendant currently owns and/or services Plaintiff's home mortgage.

14. Based on representations made by Defendant, and Plaintiff's reliance on such representations, Plaintiff believed Defendant had implemented and maintained reasonable security and practices to protect his PII. Relying on Defendant's representations and his belief that his PII would be reasonably safeguarded, Plaintiff provided his PII to Defendant in connection with receiving services from Defendant.

15. Plaintiff takes great care to protect his PII. If Plaintiff had known that Defendant does not adequately protect the PII in its possession, he would not have agreed to entrust Defendant with his PII.

16. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

17. Defendant is a limited liability company which maintains a headquarters and/or principal place of business in the Henderson, Nevada, and regularly conducts business nationwide and within this district.

## FACTUAL ALLEGATIONS

### *PII Is a Valuable Property Right that Must Be Protected*

18. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[2]

19. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[3] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

20. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[4]

21. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying

---

[2] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[3] *See* Soma, *Corporate Privacy Trend, supra*.

[4] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

22. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[5] This business has created a new market for the sale and purchase of this valuable data.[6]

23. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

24. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[8]

25. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[5] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[6] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

[7] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[8] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

***Theft of PII Has Grave and Lasting Consequences for Victims***

26. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

27. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

28. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10]

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[11] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other

---

[9] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[10] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[11] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer, or taxpayer identification number." *Id*.

things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[12]

30. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

31. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[14] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[15] And in 2019, Javelin Strategy & Research compiled consumer

---

[12] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[13] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft.

[14] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[15] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[16]

32. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

33. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[17]

34. It is within this context that Plaintiff and thousands of similar individuals must now live with the knowledge that their PII is forever in cyberspace, putting them at imminent and continuing risk of damages, and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

***Defendant's Business and their Collection of PII***

35. In providing its loan and financial services, Defendant collects sensitive personal information from customers. This information includes name, email address, username, password, social security number, phone number, mailing address, financial information and history, employment information drivers' license information, and other personal and highly sensitive personal information a person might provide when trying to procure or maintain their home loan or mortgage.

---

[16] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[17] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

Defendant hosts a large repository of sensitive personal information for its customers, including Plaintiff and the Class members.

36. Defendant knew that they needed to protect customers' PII and committed to protecting such data.

37. Plaintiff and the Class members are current or former customers of Defendant and entrusted Defendant with their PII, including but not limited to the PII compromised by the Data Breach.

***The Data Breach***

38. On or around March 6, 2024, Plaintiff received a "NOTICE OF POTENTIAL DATA BREACH" from Defendant indicating that an unauthorized party had accessed and removed data certain files from Defendant's systems, which involved Plaintiff's PII data entrusted to Defendant, including Plaintiff's name, address, social security number, and unique Nations Direct loan number.

39. In addition to the direct notice to Plaintiff and other similarly situated Class members, Defendant posted a similar notice of the Data Breach on its website.[18]

40. Defendant's NOTICE OF POTENTIAL DATA BREACH did not specify how many individuals were affected by the Data Breach, however, Defendant has announced via its reporting to the Office of the Maine Attorney General[19] that a total of 83,108 individuals nationwide were affected by the Data Breach.

41. Defendant have not shared many details regarding the cause of the Data Breach and its impact; however, the omission of an affirmative statement that the PII was encrypted and the fact that notice was provided to the California Attorney General,[20] which requires that a sample copy of a breach notice sent to more than 500 California residents, suggests that the PII was stored in the database unencrypted, or

---

[18] *See* https://myndm.com/notice-of-potential-data-breach/

[19] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1ee1929d-4e0f-4b9e-b202-59cb6d9e567d.shtml

[20] *See* sample notice of the Data Breach submitted to the California Attorney General on or around March 14, 2024: https://oag.ca.gov/ecrime/databreach/reports/sb24-582463

insufficiently encrypted, and over 500 California residents were sent notice of the Data Breach. Cal. Civ. Code § 1798.82(a)(1), requires a data breach to be disclosed to residents of California "(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable."

42. Although Defendant had knowledge of the Data Breach since December 2023, Defendant failed to notify Plaintiff and the Class members until several months later. Defendant's notice of the Data Breach was untimely, inadequate, and failed to provide sufficient detail to Plaintiff and the Class members about what PII was accessed, by whom, and for what purpose.

43. Defendant's failure to promptly notify Plaintiff and Class members that their PII was accessed and stolen by unauthorized third parties allowed those who were able to obtain their PII to monetize, misuse, or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the Class members were unable to adequately protect themselves against identity theft and fraud. Further, Plaintiff and the Class members will continue to suffer indefinitely from the damage of substantial, imminent, and concrete risk that their identities will be, or already have been, stolen and misused by unauthorized third parties.

44. As a result of the Data Breach and Defendant's conduct and/or omissions, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the unauthorized disclosure and theft of their PII; (iii) out-of-pocket

expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security to reasonably safeguard Plaintiff and the Class members' PII from unauthorized disclosure, access, and exfiltration.

## CLASS ALLEGATIONS

45. Plaintiff brings this action on behalf of himself individually and on behalf of all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure.

46. Plaintiff seeks to represent the following **Nationwide Class**:

> All individuals whose PII was subjected to the Data Breach, including all individuals who were sent a notice by or on behalf of Defendant related to the December 30, 2023 Data Breach,

47. Plaintiff also seeks to represent the following **California Sub-Class**:

> All individuals in California whose PII was subjected to the Data Breach, including all individuals who were sent a notice by or on behalf of Defendant related to the December 30, 2023 Data Breach.

48. The Class is comprised of the Nationwide Class and the California Sub-Class defined above.

49. Excluded from the Class are: (1) Defendant and their respective officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

50. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court makes a determination regarding whether certification is appropriate.

51. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

52. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of tens of thousands of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

53. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

54. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

b) Whether Defendant had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

c) Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

d) Whether Defendant breached their duty to protect the PII of Plaintiff and each Class member; and

e) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

55. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representatives of the Class in that Plaintiff have no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection and consumer privacy class actions of this nature.

56. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

57. Defendant have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final

injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

## CAUSES OF ACTION

### COUNT I

### Violation of the California Consumer Privacy Act of 2018 ("CCPA")

### Cal. Civ. Code §§ 1798.100, et seq.

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[21]

60. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

61. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to]

---

[21] *See* California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/. (last visited Aug. 14, 2023).

require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

62. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

63. Plaintiff and other similarly situated California Sub-Class members, are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017.

64. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells, or shares for

> commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

65. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and other Class members' unencrypted name, address, social security number, and unique Nations Direct loan number, among other personal information.

66. Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure because Plaintiff's PII, including name, address, social security number, and unique Nations Direct loan number, at minimum, were wrongfully accessed and taken by unauthorized persons in the Data Breach.

67. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

68. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff, individually and on behalf of the Class, seeks actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

69. On or about March 28 2024, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). In the event Defendant does not cure the violation within 30 days, Plaintiff intends to amend the operative complaint to pursue statutory damages as permitted by Civil Code

§ 1798.150(a)(1)(A).

70. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

**COUNT II**

**Negligence**

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. Defendant owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class. This duty arises from multiple sources.

73. Defendant owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendant's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Defendant controlled their technology, infrastructure, and cybersecurity, and had the duty to safeguard Plaintiff and the Class members' data, including PII.

74. Defendant further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Defendant knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

75. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect

Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant failing to use reasonable measures to protect sensitive data. Defendant, therefore, were required and obligated to take reasonable measures to protect data they possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect sensitive personal information. By failing to implement reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

76. Also, as alleged in further detail below, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, imposes an affirmative duty on businesses, such as Defendant, which maintain personal information about California residents, to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach impacting Plaintiff's and the Class members' sensitive personal information, including PII.

77. Defendant is obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

78. Finally, Defendant assumed the duty to protect sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it lawfully complied with data security requirements and had adequate data security measures in place to protect the confidentiality of Plaintiff's and the Class's private and sensitive personal information.

79. Defendant breached their duty to Plaintiff and the Class by implementing inadequate and/or unreasonable data security measures that they knew

or should have known could cause a Data Breach. Defendant knew or should have known that hackers might target sensitive data Defendant solicited and collected, which was later collected and stored by Defendant, on customers and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Defendant acknowledged they were subject to certain standards to protect data and utilize other industry standard data security measures.

80. Defendant was fully capable of preventing the Data Breach. Defendant knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach.

81. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

82. Plaintiff and the Class members have suffered damages as a result of Defendant's negligence, including actual and concrete injuries and will suffer additional injuries in the future, including economic and non-economic damages from invasion of privacy, costs related to mitigating the imminent risks of identity theft, time and effort related to mitigating present and future harms, actual identity theft, the loss of the benefit of bargained-for security practices that were not provided as represented, and the diminution of value in their PII.

**COUNT III**

**Negligence Per Se**

83. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

84. Defendant's unreasonable data security measures constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires

businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

85. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect users' sensitive data.

86. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature and amount of data Defendant stored on their users and the foreseeable consequences of a Data Breach should Defendant fail to secure their systems.

87. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

88. In addition, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq*. requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

89. Defendant violated the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures and practices to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

90. Plaintiff and the Class are within the class of persons Section 5 of the

FTC Act, the CCPA, and other similar state statutes, was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act. The CCPA, and other similar state statutes, was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

91. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

**COUNT III**

**Breach of Implied Contract**

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. Defendant provides or provided mortgage services to Plaintiff and Class members. Plaintiff and Class members formed an implied contract with Defendant regarding the provision of those services through its collective conduct, including by Plaintiff and Class members providing their PII to Defendant in exchange for the services offered.

94. Through Defendant's offering of these services, it knew or should have known that it needed to protect Plaintiff's and Class members' confidential PII in accordance with their own policies, practices, and applicable state and federal law.

95. As consideration, Plaintiff and Class members turned over valuable PII relying on Defendant to securely maintain and store their PII in return and in connection with their services.

96. Defendant accepted possession of Plaintiff's and Class members' PII for the purpose of providing services, including data security, to Plaintiff and Class members.

97. In delivering their PII to Defendant in exchange for their services, Plaintiff and Class members intended and understood that Defendant would

adequately safeguard their PII as part of those services.

98. Defendant's implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

99. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

100. Had Defendant disclosed to Plaintiff and the Class that they did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including but not limited to Defendant's decision to continue to collect, store, and maintain Plaintiff's and Class members' PII, Plaintiff and Class members would not have agreed to provide their PII to Defendant.

101. As providers of lending and mortgage servicing operations, Defendant recognized (or should have recognized) that Plaintiff's and Class member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

102. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its vendors, business associates, and/or suppliers to secure Plaintiff's and Class members' PII.

103. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide their accurate and complete sensitive personal information to

Defendant in exchange for Defendant agreement to, *inter alia*, protect their PII.

104. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

**COUNT IV**

**Unjust Enrichment**

105. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

106. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendant with their PII, which PII has inherent value. In exchange, Plaintiff and Class members should have been entitled to Defendant's adequate protection and supervision of their PII, especially in light of their special relationship.

107. Defendant knew that Plaintiff and Class members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

108. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

109. Defendant acquired the PII through false promises of data security and/or inequitable record retention as it failed to disclose the inadequate data security practices, procedures, and protocols previously alleged.

110. If Plaintiff and Class members had known that Defendant would not use adequate data security practices, procedures, and protocols to secure their PII, they would have endeavored to make alternative mortgage servicing choices that excluded Defendants.

111. Under the circumstances, it would be unjust for Defendant to be

permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

112. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

113. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from their wrongful conduct alleged herein. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

114. Plaintiff and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

//

//

**COUNT V**

**Declaratory Relief**

115. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

116. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

117. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

118. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continue to owe a legal duty to secure the sensitive personal information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendant breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendant's breach of their legal duty continues to cause harm to Plaintiff and the Class.

119. The Court should also issue corresponding injunctive relief requiring

Defendant to employ adequate security protocols consistent with industry standards to protect its users' data.

120. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

121. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

122. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

## PRAYER FOR RELIEF

123. Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class(es), (iii) Plaintiff's counsel be appointed as counsel for the Class.

124. Plaintiff, individually and on behalf of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendant including the following:

- actual and punitive damages to be determined by the trier of fact;
- equitable relief, including restitution, as may be appropriate;

- injunctive relief, including remedial measures to be implemented by Defendant designed to prevent such a data breach by adopting improved data security practices necessary to safeguard Plaintiff and the Class members' PII and extended identity theft protection and credit monitoring services design o protect Plaintiff and the Class members from identity theft and fraud;
- declaratory relief, as may be appropriate;
- pre- and post-judgment interest at the applicable legal rates;
- attorneys' fees, litigation expenses, and costs of suit; and
- any such other and further relief the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

125. Plaintiff hereby demands a jury trial on all issues so triable.

DATED this 28th day of March 2024.

Respectfully submitted,

**KAZEROUNI LAW GROUP, APC**

By: */s/ Mona Amini*

Gustavo Ponce, Esq.
Mona Amini, Esq.
6787 W. Tropicana Ave., Suite 250
Las Vegas, Nevada 89103

*Attorneys for Plaintiff*